SPC

Sistema Pubblico di
Connettività e Cooperazione

COMMISSIONE DI COORDINAMENTO SPC

CONTENUTI DELLE GARE S2 E S3

versione 1.0

DigitPA

INDICE

DigitPA

1. PREFAZIONE

1.1. Componenti del gruppo di lavoro

Francesco Tortorelli (Coordinatore)	DigitPA
Francesco Caputo	DigitPA
Marino Di Nillo	DigitPA
Domenico Davide Lamanna	DigitPA
Giorgia Lodi	DigitPA

Annalisa Mannucci	Comune di Roma
Federica Silvestrini	Ministero dell'economia e delle finanze
Caterina Cirmi	Comune di Roma
Ertini Geremia	Regione Basilicata
Paolo Boscolo	Comune di Prato
Marialaura Maggiulli	Regione Marche
Giorgio Maddalena	Datasiel (Regione Liguria)
Maurizio Carlin/Boni	Comune di Venezia
Marcello Niceforo	Ministero dell'economia e delle finanze
Pietro Romanazzi	Regione Puglia
Federica Brazzafolli	Comune di Pordenone
Valentino Di Toma	Ancitel
Rosa Rosini	Ministero della Salute
Dorotea Alessandra De Marco	Ministero della Salute
Andrea Nicolini	Cisis

1.2. Modifiche Documento

Descrizione Modifica	Edizione	Data
Definizione della ToC	0.1	21/09/2011
Inserimento delle figure 1,2 e 3	0.2	09/10/2011
Prima revisione delle figure e del documento	0.3	10/10/2011
Seconda revisione delle figure e del documento	0.4	16/10/2011
Revisione completa del documento	0.6	11/11/2011
Seconda revisione completa del documento	0.8	17/11/2011
Emissione definitiva	1.0	21/11/2011

1.3. Acronimi

Acronimo	Definizione
CAD	Codice dell'Amministrazione Digitale
SPC	Sistema Pubblico di Connettività
SPI	Software, Piattaforma, Infrastruttura
Q-ISP	Qualified Internet Service Provider
Q-ASP	Qualified Application Service Provider
PA	Pubblica Amministrazione
GFID	Gestione Federata Identità Digitali
ULS	Unità Locali di Sicurezza
SOC	Security Operation Centre
CAPEX	CAPital Expenditure – Spese in conto capitale
OPEX	OPerating Expense – Spese di esercizio
CERT-SPC-C	CERT-SPC Centrale
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
REST	Representational State Transfer
CIE	Carta d'Identità Elettronica
CNS	Carta Nazionale dei Servizi
SAML	Security Assertation Markup Language
HTTP	HyperText Transfer Protocol
XML	eXtensible Markup Language
AAA	Authentication, Authorization, Accounting

2. SCOPO DEL DOCUMENTO

Secondo quanto discusso dalla Commissione di Coordinamento (CdC) SPC, il presente documento ha lo scopo di definire i contenuti delle gare S2 e S3 per i futuri servizi del Sistema Pubblico di Connettività (SPC), in attuazione delle norme introdotte dal nuovo Codice dell'Amministrazione Digitale (CAD), D.Lgs. n. 235 del dicembre 2010. La Commissione di Coordinamento ha definito 4 ambiti di servizi: S0-Servizi infrastrutturali per l'interoperabilità e la cooperazione tra sistemi informativi di più PA; S1-Servizi di connettività e di infrastruttura di base; S2-Servizi interattivi per utenti finali; S3-Servizi per sistemi informativi interni alla singola PA orientati alla federabilità delle PA.

Il documento rappresenta pertanto una linea di indirizzo per gli organismi di attuazione e controllo, come definiti all'art. 1, lettera hh), dell'allegato al DPCM 1 aprile 2008, recante "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'art. 71, comma 1 bis del decreto legislativo 7 marzo 2005, n. 82".

3. TIPOLOGIA DI DOCUMENTO

Il presente documento rappresenta un documento di LINEE GUIDA relativo alla "*promozione dell'evoluzione del modello organizzativo e dell'architettura tecnologica del SPC in funzione del mutamento delle esigenze delle pubbliche amministrazioni e delle opportunità derivanti dalla evoluzione delle tecnologie*", come specificato all'art. 79, comma 2, lettera c) del CAD, che definisce i compiti della Commissione di coordinamento SPC.

Il documento è destinato agli organismi di attuazione e controllo SPC e a tutte le pubbliche amministrazioni.

4. QUADRO D'INSIEME: IL FRAMEWORK SPC

Nell'attuazione del nuovo SPC (come del resto di tutto il CAD) è necessaria un'azione congiunta di un più ampio insieme di attori che vanno dalle PA, ai cittadini e imprese, fino al mercato con una sua apertura sia verso i grandi e consolidati player ma anche verso più piccole realtà.

La Figura 1 illustra il quadro d'insieme del framework SPC con i principali attori coinvolti ai sensi dell'art. 75 del nuovo CAD.

SPC e i suoi principali attori. Il framework è conforme alla definizione di SPC data dall'art. 73 del nuovo CAD che lo identifica come *"l'insieme di infrastrutture tecnologiche e regole tecniche per lo sviluppo, condivisione, integrazione e diffusione del patrimonio informativo e dei dati delle PA […] garantendo la sicurezza, la riservatezza delle informazioni nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna PA"*.

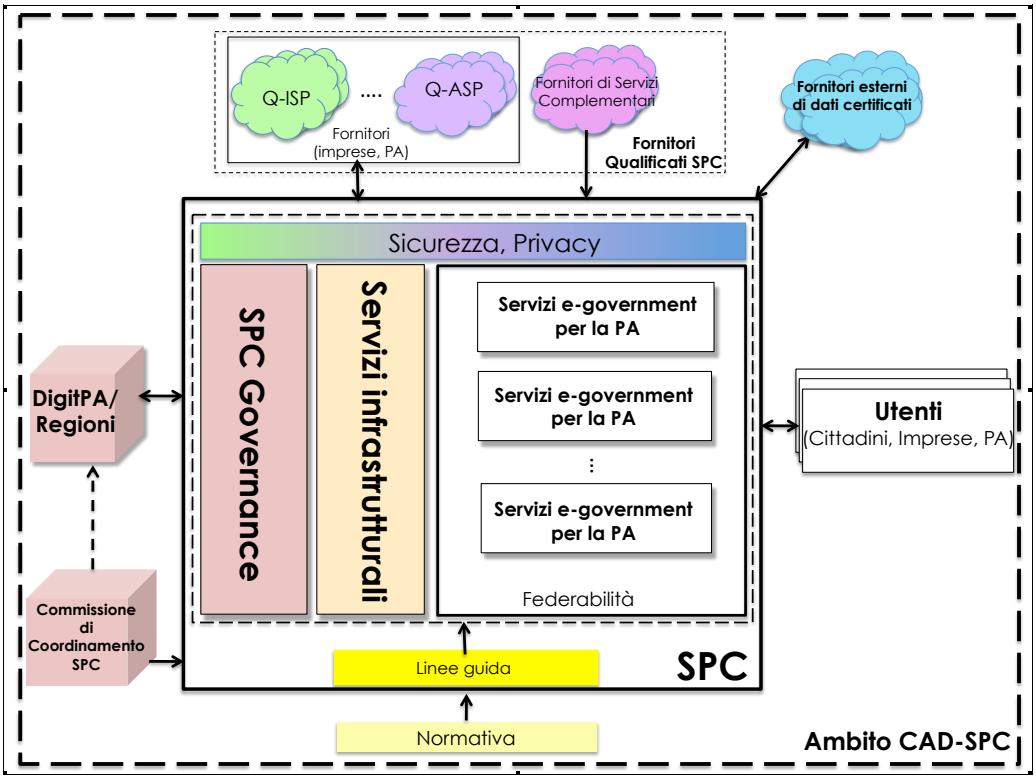

Figura 1: Il framework SPC e i suoi principali attori

Partendo dalla normativa nazionale vigente e dalle direttive internazionali, per esempio la Digital Agenda già identificata nel documento sugli obiettivi delle gare S2 e S3, regole tecniche e linee guida costituiscono le fondamenta del framework, in quanto driver per lo sviluppo sia di servizi specifici di cui le PA si possono dotare per proporre e, utilizzare esse stesse, servizi evoluti e *aggregati* di e-government (in Figura 1 i "silos" chiamati servizi e-government per la PA), sia dell'insieme di

infrastrutture nazionali condivise a supporto di tali servizi specifici (in Figura 1 i cosiddetti servizi infrastrutturali).
I servizi infrastrutturali e quelli specifici per le PA sono utilizzati e offerti, rispettivamente, da un insieme di fornitori qualificati SPC. I fornitori qualificati SPC si distinguono in imprese ICT che operano sul mercato come Internet Service Provider o Application Service Provider, e le PA stesse che potrebbero al loro interno fornire servizi verso altre PA (anche nell'ottica dei principi di riuso del software chiaramente identificati negli obiettivi delle future gare e regolati all'art. 69 del nuovo CAD).
Questi fornitori, per accedere al perimetro SPC con i loro servizi, devono essere soggetti alla procedura attualmente prevista di certificazione e qualificazione. A tal riguardo essi vengono denominati Qualified Internet Service Provider e Qualified Application Service Provider (Q-ISP, Q-ASP in Figura 1).
Oltre a questa categoria, recenti modifiche al CAD aprono a nuovi scenari per i fornitori qualificati SPC. In particolare, all'art. 75 si prevede che anche soggetti privati che operano con finalità pubbliche possono parteciparvi, previa particolare procedura di qualificazione e accreditamento degli stessi definita dalla Commissione di Coordinamento SPC. In Figura 1 tali fornitori sono detti *fornitori di servizi complementari*: possono infatti rientrare in questa categoria tutti quei soggetti privati che offrono servizi a complemento degli esistenti. Per esempio, le banche e/o poste usate dalle PA per i servizi di pagamento possono essere considerati fornitori di servizi complementari.
Infine, esistono fornitori che non rientrano all'interno del perimetro SPC, e pertanto non sono soggetti a procedure di qualificazione e accreditamento. Tali fornitori, chiamati *Fornitori esterni di dati certificati*, possono essere di supporto ad alcuni servizi specifici SPC per l'erogazione di dati certificati in loro possesso. Nella gestione federata delle identità (GFID), le external attribute authority, come ad esempio gli ordini professionali, sono considerate fornitori esterni di dati certificati.

SPC governance. L'intera governance di SPC è attribuita alla Commissione di Coordinamento, la cui presidenza è affidata a DigitPA. La Commissione ha il compito di approvare le linee guida e tutte le procedure che riguardano le attività svolte nel contesto SPC. DigitPA, e le Regioni per quel che riguarda la loro autonomia locale, sono responsabili della governance sia dei servizi infrastrutturali sia dei contratti quadro in cui vengono definiti i servizi e-government per la PA.

Servizi SPC. I servizi offerti da SPC si distinguono in servizi infrastrutturali e servizi specifici e-government per la PA. I servizi e-government per la PA sono l'insieme di servizi utilizzati dalle singole PA per la gestione dei loro back-office e per fornire prestazioni evolute ai cittadini e imprese, nonchè ad altre PA.
I servizi infrastrutturali invece consistono nell'insieme di risorse SPC necessarie per supportare comunicazioni sicure e fidate, l'interoperabilità e cooperazione applicativa tra le Pubbliche Amministrazioni. Mediante l'utilizzo di tali infrastrutture, l'interoperabilità tra diversi sistemi delle PA può essere garantita a ogni livello di astrazione, dalla connettività fino al livello applicativo.

Federabilità. A tal riguardo, è importante notare che i servizi infrastrutturali sono cruciali per realizzare integralmente la cosiddetta *federabilità* dei servizi e-government per la PA (come mostrato in Figura 1). Il ridisegno del CAD porta a considerare la federabilità dei sistemi informativi della Pubblica Amministrazione un requisito indispensabile per la creazione e l'erogazione di un insieme di servizi aggregati e pro-attivi agli utenti finali. In virtù dei principi sanciti già dalla legge 241/90 e poi ripresi dal CAD, il cittadino e/o l'impresa hanno il diritto di *non* fornire alle PA *più volte* un dato che esse già

possiedono, conseguentemente anche la federabilità tra i servizi e-government per la PA diventa requisito strategico e basilare nel ridisegno SPC. Il nuovo modello di principio per i servizi del SPC si propone di recepire i paradigmi ICT dei sistemi aperti, distribuibili e federati per poter mettere i suoi utenti finali (PA, cittadini e imprese) nelle condizioni di esercitare tali diritti.
La natura federata del SPC è infatti uno dei principi realizzativi enunciati all'art. 73, comma 3, lett. a) del CAD.
Quanto sopra ricordato ha un chiaro impatto sull'identificazione degli ambiti di fornitura delle future gare che dovranno includere un insieme di servizi specifici a supporto della federabilità finalizzati ad esempio a garantire la qualità e certificazione del dato, la comunicazione tra servizi e-government di diverse PA, ecc.

Sicurezza e privacy. Nell'erogazione dei servizi SPC, requisiti di sicurezza e privacy devono essere garantiti a tutti i livelli. Sono previsti quindi opportuni servizi di sicurezza e di privacy sia a livello di infrastrutture di connettività sia a livello applicativo tali da consentire lo svolgimento di operazioni di back office e front office complesse in maniera sicura e nel rispetto della vigente normativa in materia di privacy dei dati.
Da un punto di vista organizzativo, la governance SPC rafforza la gestione della sicurezza mediante l'istituzione e il consolidamento del Centro denominato CERT-SPC-C. Tale centro ha lo scopo di monitorare e analizzare, attraverso opportune correlazioni, tutti i dati riguardanti incidenti di sicurezza verificatisi all'interno delle Pubbliche Amministrazioni. Per rendere operative tali operazioni del centro, le singole Pubbliche Amministrazioni, siano esse locali o centrali, si dotano di Unità Locali di Sicurezza (ULS).
Le ULS hanno il compito di cooperare con il CERT-SPC-C inviandogli regolarmente dati relativi a incidenti (per esempio attacchi cyber o minacce di altro tipo); il centro, grazie alla complessa correlazione che svolge sui dati, riesce tempestivamente a informare le Amministrazioni su eventuali attacchi in essere. Le ULS possono avvalersi dei Security Operation Centre (SOC) dei propri fornitori qualificati SPC per svolgere il compito suddetto a loro assegnato. In sostanza, ogni Amministrazione dovrà dotarsi di opportuni servizi di sicurezza a supporto delle attività delle ULS. Essi verranno identificati nell'insieme degli ambiti di fornitura così come descritto nella Sezione 7 del presente documento.

In generale, è da sottolineare che l'evoluzione di SPC non può essere confinata solo a specifici settori ma coinvolge indistintamente tutti i suoi livelli di astrazione fin qui descritti e illustrati in Figura 1. Tuttavia, questo documento si focalizza solo sul nuovo modello di erogazione dei servizi e-government per la PA, dettagliando i principali ambiti di fornitura che rientrano in tale categoria e che consentono di determinare i servizi oggetto della futura gara applicativa.

5. MODELLI DI SERVIZIO

Come sottolineato in [1], il mercato attualmente offre un nuovo modello di business dove capacità IT scalabili e altamente flessibili sono fornite *come servizio* a uno svariato numero di utenti utilizzando tecnologie basate su Internet. Tale modello abilita accessi facilitati multicanale e disponibili in qualunque momento a un vasto pool di risorse di computazione *configurabili* e *condivise*, che vanno dalle risorse fisiche di rete, di storage e di processamento ai servizi fino alle applicazioni finali di front end, e che sono flessibilmente e rapidamente erogabili con minimi sforzi di gestione.

Al fine di rispondere efficacemente agli obiettivi identificati in [1] e ridurre i costi di gestione e manutenzione del comparto dei servizi e-government per la PA, così come attualmente è auspicabile realizzare, questo documento propone *un'evoluzione* del modello di servizio attualmente impiegato in SPC verso un modello che rispecchi pienamente le suddette caratteristiche e che possa essere preso quindi come riferimento per la fornitura dei futuri servizi e-government per la PA. Occorre tener conto che le esigenze di federabilità sono funzionali anche ai principi di gestione aggregata dei servizi che trovano riscontro tanto a livello locale quanto centrale; in entrambi i casi la normativa e ancora più spesso esperienze pratiche hanno messo in campo soluzioni condivise di risorse e di servizi.

La Figura 2 mostra tale evoluzione. Nell'attuale SPC il modello di gestione impiegato per i servizi specifici e-government delle PA prevede due possibili soluzioni: le cosiddette soluzioni in house o quelle di hosting. Nel caso di soluzioni in house le risorse hardware, connettività, software e l'insieme di tutti i servizi offerti agli utenti finali risiedono tipicamente presso il data center delle Pubbliche Amministrazioni con conseguente completo controllo e responsabilità ben definite sulle stesse, ma anche una capacità di erogazione fissa e più alti costi per la loro acquisizione, gestione e manutenzione (ossia alti costi CAPEX e OPEX).

Soluzioni di hosting consentono invece una maggiore flessibilità. In questo caso, le Pubbliche Amministrazioni possono affittare risorse hardware, connettività, software e servizi con conseguente minor controllo e responsabilità su di esse e minori costi iniziali per acquisirle (minori CAPEX). Tuttavia, ancora una volta, le capacità di erogazione dei servizi offerte da soluzioni di tipo hosting sono per la maggior parte dei casi fisse e non flessibili, con possibili risorse anche inutilizzate per diversi periodi.

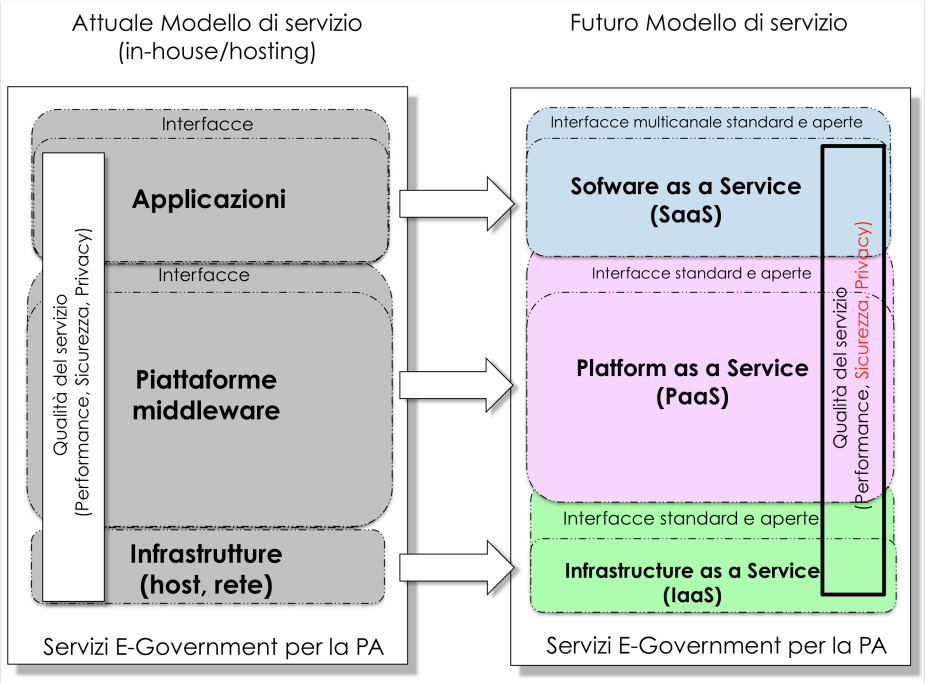

Figura 2: Evoluzione del modello di servizio per i servizi e-government per la PA

Il futuro modello di riferimento SPC per i servizi e-government per la PA consente di sfruttare i vantaggi attualmente offerti da soluzioni di hosting ai quali aggiungere però maggiore flessibilità nella gestione ed erogazione dei servizi stessi. Nel nuovo modello, l'infrastruttura hardware e software è "multi-tenant" (ovvero in multi-proprietà) e condivisa tra più utenti e le risorse sono gestite in pool così da garantire risparmio e alta scalabilità anche a fronte di un più elevato numero di accessi ai servizi in rete. Le risorse infatti vengono assegnate e riassegnate a seconda dell'effettiva domanda.

Il nuovo modello fornisce inoltre capacità di erogazione dinamiche, abilitando modelli di pricing "a consumo". In particolare, le Pubbliche Amministrazioni possono sfruttarlo indipendentemente dalla topologia di rete, pagando solo per l'effettivo consumo, con un possibile risparmio sui costi di acquisizione e conduzione (riduzione o azzeramento dei CAPEX e riduzione degli OPEX). In questo contesto, il nuovo modello di servizio SPC può essere vantaggiosamente impiegato in tutti quegli scenari che richiedono alta affidabilità e scalabilità degli accessi, necessaria per le transazioni G2C (Government-to-Citizen), alta flessibilità per la gestione di carichi variabili e integrazioni tra più servizi necessaria nelle interazioni G2G (Government-to-Government).

E' facile notare da queste premesse che, mentre nel passato si dovevano espressamente prevedere meccanismi trasversali a garanzia di requisiti di Qualità del Servizio come performance, scalabilità, sicurezza e privacy, nel nuovo modello alcuni di questi requisiti (e.g., scalabilità, efficienza, performance) sono "nativamente" supportati, grazie alla maggiore flessibilità che lo stesso modello offre. Tuttavia, attenzione particolare deve essere riservata ai requisiti di sicurezza e privacy che emergono in maniera significativa a fronte delle funzionalità di multi-tenancy. Il modello attuale, a determinati livelli di astrazione, risulta ancora poco maturo per quanto riguarda la sicurezza e la

riservatezza dei dati; pertanto devono essere esplicitamente previsti opportuni servizi in grado di garantire tali requisiti (Sezione 7).

Il nuovo modello (mostrato nel lato destro di Figura 2) viene anche chiamato modello SPI, di fornitura di servizi Software, Piattaforma e Infrastrutturali. L'enfasi non è più sul prodotto ma quanto sul servizio. Esso è basato sul concetto di "pila" a tre livelli: il livello infrastrutturale nella parte inferiore della pila, il livello software nella parte superiore e quello piattaforma in mezzo.

Il livello infrastrutturale (IaaS) permette di avere risorse di elaborazione quali potenza di calcolo, storage e segmenti di rete. In tale livello rientrano poi quell'insieme di servizi che consentono il controllo sulla configurazione dei sistemi e dei servizi di base a bordo delle risorse noleggiate. Il livello IaaS offre il maggior grado di estendibilità in quanto costituisce il "primo mattone" sul quale poi ospitare i servizi piattaforma e quelli di livello software per l'utilizzo da parte degli utenti finali.

Il livello piattaforma (PaaS) offre la piattaforma e l'ambiente di sviluppo applicativo (run time) come un vero e proprio servizio grazie al quale ospitare e distribuire applicazioni terze del livello soprastante.

Infine, il livello software (SaaS) offre, sottoforma di servizi, tutte quelle applicazioni software che sono accessibili da parte degli utenti finali in qualunque momento e avvalendosi di diversi dispositivi (dai normali desktop e server, ai dispositivi mobili come cellulari e tablet). Questo livello offre il minor grado di estensibilità per il fruitore finale rispetto ai precedenti in quanto gli utilizzatori potranno usufruire in modo trasparente di tutte le funzionalità di gestione e controllo offerte dai livelli IaaS e PaaS; i fruitori delle applicazioni potranno opportunamente configurarle sulla base delle specifiche necessità dei loro utenti finali.

Ogni livello della pila espone al livello soprastante un insieme di interfacce. Le interfacce sono aperte, possibilmente multicanale basate su standard ben definiti (come mostrato in Figura 2) così da consentire un accesso ubiquo, unificato e affidabile a una vasta pletora di servizi (per maggiori dettagli si veda la Sezione 6.2), nonché un forte riuso e interoperabilità.

5.1. Responsabilità: erogatore e fruitore di servizi

Le Pubbliche Amministrazioni possono adottare il modello in veste sia di fruitore di servizi, sia di erogatore.

In qualità di fruitore di servizi, le Pubbliche Amministrazioni non hanno responsabilità e particolari oneri per quel che riguarda l'acquisizione, la gestione ordinaria e straordinaria delle risorse, delle piattaforme e dei servizi. Esse possono utilizzare i servizi con costi strettamente correlati al reale fabbisogno e utilizzo, demandando all'erogatore tutte quelle responsabilità che coinvolgono necessariamente la gestione flessibile delle risorse (prevedendo anche meccanismi di disaster recovery e business continuity) e dei servizi di base, richiesti per far fronte alle diverse esigenze di carichi variabili dei fruitore.

In qualità di erogatore di servizi, le PA assumono inevitabilmente quegli oneri che riguardano la gestione delle infrastrutture e dei relativi servizi. Da notare come Pubbliche Amministrazioni possono assumere il ruolo di erogatori non solo per se stessi ma anche per altre Pubbliche Amministrazioni. Quest'ultimo scenario potrebbe portare ad incentivare e favorire la pratica di riuso del software, così come sancito all'art. 69 del nuovo CAD e dagli obiettivi delle future gare [1].

Tuttavia, il modello proposto in Figura 2 è sufficientemente flessibile per lasciare alti gradi di libertà alle Pubbliche Amministrazioni nella scelta di quali livelli del modello effettivamente adottare come meri fruitori o come erogatori. Così, un'Amministrazione potrebbe dotarsi solo dei servizi di livello IaaS, esercitando quindi un pieno controllo sui livelli PaaS e SaaS soprastanti. Questo scenario potrebbe essere applicato sia nel caso di Pubbliche Amministrazioni non in grado di poter acquisire tutte quelle risorse necessarie per il dispiegamento di un proprio data center sul quale ospitare le proprie applicazioni, sia nel caso di Pubbliche Amministrazioni che vogliono rinnovare i propri data center ed eventualmente fungere poi da erogatori per altre pubbliche amministrazioni. Alternativamente le Pubbliche Amministrazioni possono agire come fruitori dei livelli PaaS e SaaS, concentrandosi solo sugli aspetti più funzionali della logica applicativa, oppure utilizzare tutti i servizi, di tutti i livelli, offerti da altri erogatori.

Questa flessibilità ha conseguentemente un impatto sulle reali responsabilità che le diverse Pubbliche Amministrazioni possono assumersi.

La Figura 3 illustra tali responsabilità e come queste evolvono nel caso di precedenti soluzioni in house e nel caso di nuove soluzioni che sfruttano il modello SPI proposto.

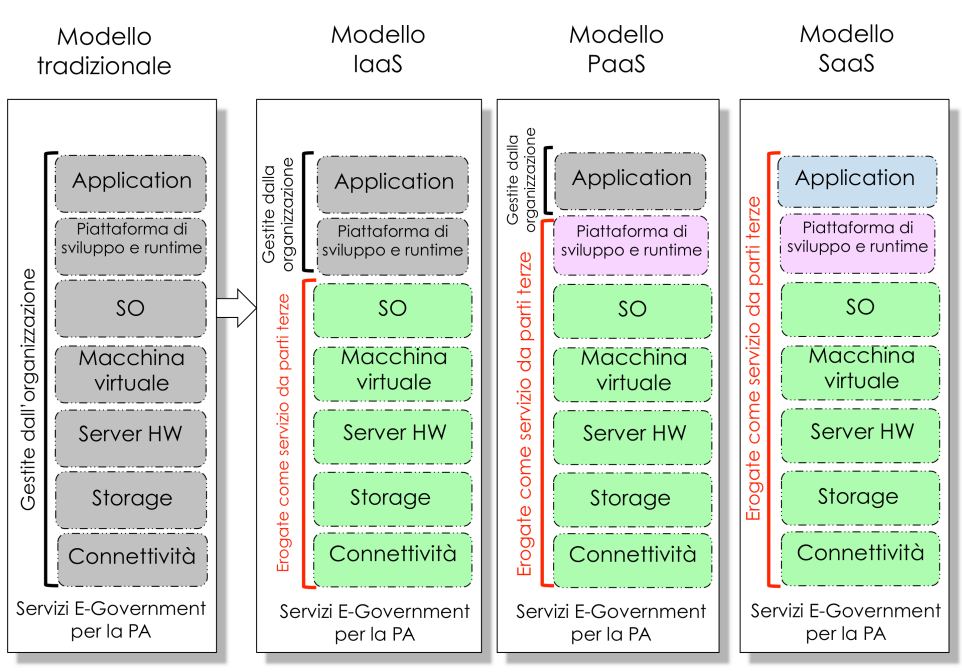

Figura 3: Evoluzione delle responsabilità verso i modelli IaaS, PaaS e SaaS

6. MODALITÀ DI DISTRIBUZIONE E DI INTERAZIONE DEI SERVIZI E-GOVERNMENT PER LA PA

6.1. Modelli di deployment

Il modello precedentemente descritto trova attualmente applicazione grazie alle cosiddette soluzioni di cloud computing. Ne esistono di svariate disponibili sul mercato che sono oramai fornite da diverse famose organizzazioni IT. In generale, queste tecnologie implementano i modelli di servizio IaaS, PaaS e SaaS e si basano sulla *virtualizzazione* per garantire le necessarie caratteristiche innovative di elasticità, flessibilità e scalabilità prima discusse. Tecnologie cloud a livello IaaS includono Amazon EC2 e S3, a livello PaaS includono Google Apps Engine e Microsoft Azure, e a livello SaaS Google Docs e Gmail, per citare alcuni tra i più comuni esempi.

Tuttavia, indipendentemente dai livelli IaaS, PaaS e SaaS, il dispiegamento dei servizi può avvenire attraverso diverse modalità. E' importante fin da subito sottolineare come alcune di queste modalità, in particolare modalità di cloud ibrido e di comunità descritte in seguito in questa sezione, risultano particolarmente adatte e vantaggiose, anche sotto un profilo economico, per il contesto della Pubblica Amministrazione. Grazie infatti a tali modalità, le PA hanno diversi gradi di libertà nell'usufruire dei benefici del modello dei servizi prima discusso, mantenendo al contempo quel controllo sui dati e sui servizi necessario in taluni casi viste la criticità del complesso delle informazioni gestite e le vigenti normative anche in materia di privacy e sicurezza.

In generale, si distinguono i seguenti modelli di deployment di servizi cloud (rif. ai documenti prodotti dal GdL sul cloud computing disponibili nei prossimi giorni):

- **Cloud pubblica**: in una cloud pubblica, i servizi sono generalmente offerti alle organizzazioni attraverso Internet. In questo modello di deployment, risorse, piattaforme e servizi sono interamente erogati e gestiti da specifici erogatori di servizi cloud (Amazon, Google, IBM, Oracle, Microsoft ne sono un esempio) che mettono a disposizione dei fruitori un'infrastruttura IT comune e condivisa capace di attuare i principi di multi tenancy, scalabilità e flessibilità tipici del modello discusso nella precedente sezione. Quando si parla di cloud pubblica, i fruitori dei servizi non hanno quindi né il controllo diretto sulla gestione dei dati e servizi, né il controllo sulla reale posizione geografica dei dati e dei servizi affidati alla cloud pubblica che potrebbero essere ospitati anche al di fuori dei confini nazionali sulla base della gestione scelta dal fornitore in quanto unico responsabile. Quest'ultima peculiarità è attualmente considerata uno dei principali limiti alla piena adozione del modello cloud pubblico: essa può essere in contrasto infatti con requisiti legislativi e di sicurezza dei dati da rispettate in taluni contesti, ivi compreso quello della Pubblica Amministrazione.
- **Cloud privata**: in una cloud privata, le risorse, piattaforme e servizi operano per una singola organizzazione. Le organizzazioni che adottano questo modello di deployment possono utilizzare i processi e le procedure esistenti adattandole a un ambiente più virtualizzato e automatico in maniera da garantire le funzionalità del cloud quali elasticità, flessibilità e scalabilità (anche se limitatamente ai confini amministrativi e tecnici dell'Amministrazione), conservando al tempo stesso controllo e sicurezza sui dati. Un cloud privato può essere implementato internamente ossia in un data center di

proprietà del fruitore dei servizi cloud, esternamente ossia in un data center di terze parti, oppure in parte internamente e in parte esternamente.

- **Cloud privata su cloud pubblica**: in una cloud privata su cloud pubblica si consente a fruitori di servizi cloud di definire una propria topologia di rete virtuale, come se essa operasse all'interno del proprio data center, al di sopra delle risorse messe a disposizione da un cloud pubblico. Il fruitore ha così pieno controllo sulla porzione a esso dedicata ad uso esclusivo; egli può così specificare e configurare opportunamente quella parte di rete virtuale a seconda dei requisiti di sicurezza richiesti. Sebbene quindi tale modalità di deployment offra un maggior controllo sulla porzione di infrastruttura dedicata, non garantisce però il pieno controllo sulla posizione geografica dell'infrastruttura stessa che è comunque gestita dall'erogatore di cloud pubblico. Quest'ultimo ha inoltre meno flessibilità di gestione rispetto a una soluzione di cloud pubblico pura in quanto la parte dedicata, quando in uso, non può essere utilizzata per altri fruitori. E' da notare che tale tipo di deployment non è largamente utilizzato e attualmente è applicato solo per il livello IaaS; Amazon Virtual Private Cloud è l'unica soluzione nota e consolidata disponibile sul mercato. Altri erogatori, come ad esempio Telecom Italia, stanno considerando comunque tale modello di deployment nelle loro future offerte IaaS.
- **Cloud di comunità**: Una cloud di comunità è una via di mezzo tra una cloud privata e una cloud pubblica. Essa quindi eredita i vantaggi di entrambi i modelli. Come nel caso del cloud pubblico, una cloud di comunità serve diversi utenti abilitando i principi di multi tenancy. Tuttavia, tali utenti non sono tra loro sconosciuti: essi tipicamente appartengono a una specifica comunità (per esempio la comunità delle Pubbliche Amministrazioni) e condividono pertanto le stesse esigenze e caratteristiche dei servizi da utilizzare. Al contrario però del modello cloud pubblico, le cloud di comunità sono costruite e operano secondo i termini stabiliti dai fruitori dei servizi: esse possono essere create in maniera tale da essere conformi, per esempio, agli standard utilizzati dagli utenti della comunità. I fruitori di una cloud di comunità pagano il fornitore per quello che realmente utilizzano così da abbattare i costi CAPEX e OPEX.
- **Cloud ibrida**: una cloud ibrida combina più di uno dei modelli precedentemente introdotti. Così, un'organizzazione potrebbe utilizzare una cloud privata per conservare il totale controllo su determinati dati considerati sensibili ma comunque collaborare con organizzazioni simili, che perseguono le sue stesse finalità, utilizzando una cloud di comunità. Alternativamente, un'organizzazione potrebbe utilizzare una cloud privata per la gestione dei propri dati e servizi proprietari e sensibili, e una cloud pubblica per la gestione di tutte quelle applicazioni e quei dati secondari che non necessitano di forti requisiti di sicurezza e riservatezza. In entrambi i casi, la flessibilità offerta da tale modello è alta, la scalabilità on demand è comunque garantita e i costi di acquisizione e gestione possono essere ridotti. Tuttavia, l'integrazione tra diversi sistemi potrebbe portare a una gestione complessa degli stessi con l'inserimento di potenziali vulnerabilità anche di sicurezza.

La Tabella 6.1 riassume le principali caratteristiche delle modalità di deployment offerte dal modello cloud, indicando alcuni esempi di sistemi attualmente offerti dal mercato.

	Cloud privata	Cloud pubblica	Cloud privata su cloud pubblica	Cloud di comunità	Cloud ibrida
Costi – CAPEX OPEX	Relativamente alti	Bassi	Bassi	Ridotti (costi ripartiti tra utenti nella comunità)	Ridotti
Sicurezza	Alta (a tutti i livelli IaaS, PaaS, SaaS, massimo controllo sui dati)	Bassa (a tutti i livelli necessario adottare opportune misure)	In parte garantita (a livello IaaS meccanismi tradizionali di sicurezza e controllo degli accessi; minori garanzie a livello di PaaS e SaaS)	In parte garantita (potrebbero esserci vulnerabilità all'interno della comunità)	Alta per i dati sensibili (più controllo sulla parte privata dove possono risiedere dati sensibili)
Privacy	Alta (a tutti i livelli IaaS, PaaS, SaaS, si possono definire le opportune politiche di privacy)	Bassa (a tutti i livelli necessario adottare opportune misure)	In parte garantita (a livello IaaS garanzie di isolamento; minori garanzie a livello di PaaS e SaaS)	In parte garantita (potrebbero esserci criticità se politiche di privacy non sono opportunamente definite e gestite tra i membri della comunità)	Alta per i dati sensibili (più controllo sulla parte privata dove possono risiedere dati sensibili opportunamente protetti secondo quanto previsto dalla vigente normativa)
Scalabilità on demand	Limitata	Sì	Sì	Sì	Sì
Ambiente multi-tenant	No	Sì	Sì (gestione poco flessibile)	Sì	Sì
Flessibilità di gestione ed erogazione dei servizi	Limitata	Massima	Limitata	Alta (gestione flessibile nel contesto ristretto della comunità)	Alta (anche se più complessa da gestire)
Responsabilità	Piena della PA (in certi casi condivisa)	Piena del fornitore cloud pubblico	Condivisa (tra la pubblica amministrazione e il fornitore cloud)	Condivisa (tra la comunità delle pubbliche amministrazioni e il fornitore cloud)	Condivisa (tra la pubblica amministrazione e il fornitore cloud)
Esempi attualmente utilizzati	• Ubuntu Enterprise Cloud • Xen Cloud Platform	• Amazon EC2 • Google Apps	• Amazon Virtual Private Cloud (VPC)	• Eucalyptus Community Cloud • GovCloud • IBM FCC	• OpenNebula

Tabella 6.1: Principali caratteristiche ed esempi dei diversi modelli di deployment

In generale, l'analisi di tali modelli conferma quanto precedentemente introdotto: sia il cloud di comunità che il cloud ibrido possono essere due tipi di dispiegamento dei servizi

particolarmente adatti e vantaggiosi per il contesto delle Pubbliche Amministrazioni, che potrebbero così sfruttare le innovative caratteristiche dei modelli di servizi descritti in Sezione 5 mantenendo allo stesso tempo un controllo sui dati e sui forti requisiti di sicurezza e riservatezza richiesti nell'ambito SPC ed e-government in generale.

6.2. Modalità di interazione

Il nuovo modello SPC di riferimento fornisce ulteriori modalità di interazione tra le organizzazioni, interazioni che consentono di realizzare quella federabilità dei sistemi informativi delle PA richiesta al fine di garantire una condivisione interoperabile e sicura delle informazioni.

In particolare, date due Pubbliche Amministrazioni, esistono due casi possibili di interazioni: (i) interazione tra due PA che utilizzano entrambe il nuovo modello SPI e (ii) interazione tra due PA in cui una utilizza il vecchio modello SPC e una schiera invece il nuovo modello, così come descritto in sezione 5.

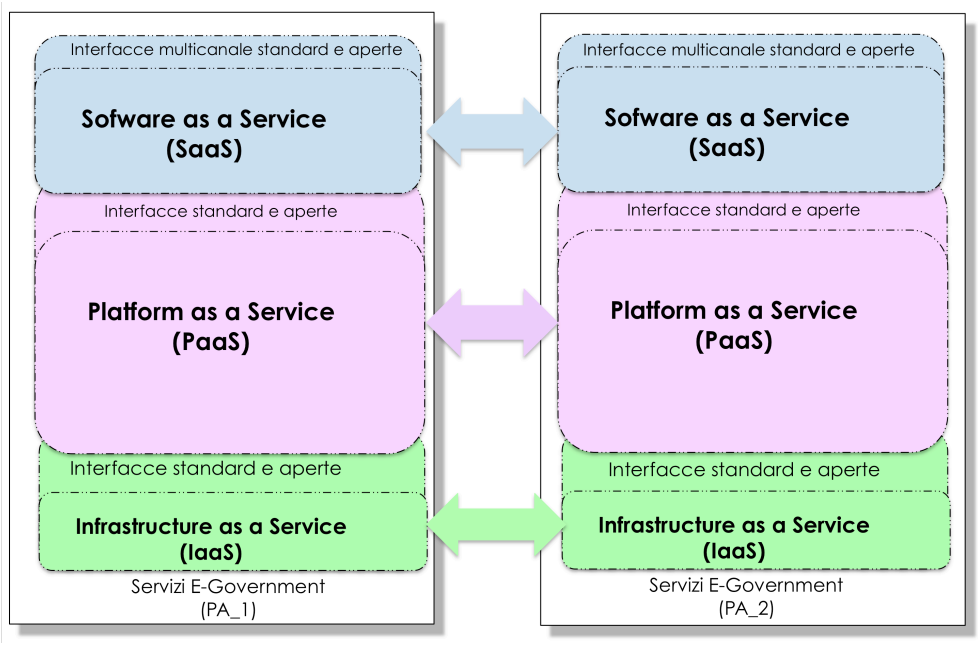

Figura 4: Interazione nel nuovo SPC

La Figura 4 mostra un'interazione tra due PA che adottano entrambe il nuovo modello SPC così come presentato in Figura 2 lato destro. Per poter abilitare tale tipo di interazione, l'interoperabilità per soluzioni SaaS, PaaS e IaaS deve essere fornita. Nel contesto cloud, tale interoperabilità non è "automatica": la vasta pletora di organizzazioni IT che offrono soluzioni di questo tipo ha fatto emergere la problematica relativa alla capacità di far interoperare tali soluzioni, problematica che risulta particolarmente sentita nei casi PaaS e SaaS. Sebbene esistano alcune infrastrutture in grado di garantire tale interoperabilità (e.g., OpenNebula), è necessario ribadire che standard (e.g., XML, SAML, HTTP) e

interfacce comuni (e.g., REST) e aperte devono essere utilizzate e implementate ad ogni livello della pila SPI. Solo in questo modo si possono avere maggiori garanzie sull'effettiva capacità di interazione dei servizi di ogni livello.

Nella seconda modalità l'Amministrazione che usa il precedente modello SPC potrà usufruire dei tradizionali elementi di cooperazione applicativa (i.e., la porta di dominio) interfacciandosi attraverso l'uso di standard ai servizi del nuovo modello.

E' opportuno far presente che il ridisegno di SPC coinvolgerà anche i servizi infrastrutturali per la cooperazione che dovranno essere ripensati nell'ottica di supportare il nuovo modello di riferimento proposto e abilitare efficacemente la federabilità dei sistemi informativi delle PA. Questo inevitabilmente comporterà la definizione di nuove regole tecniche e linee guida che dovranno definire in maniera dettagliata i meccanismi di interazione e interoperabilità per ogni nuovo livello del modello dei servizi.

6.3. Sostenibilità del modello dei servizi

I modelli di servizio, di distribuzione e interazione fin qui discussi e suggeriti per il contesto specifico dell'e-government risultano particolarmente adatti nel soddisfare l'insieme degli obiettivi funzionali e non già precedentemente introdotti nel documento [1].

In particolare, le caratteristiche di flessibilità di gestione, elasticità e scalabilità on demand offerte dal modello di riferimento consentono le Pubbliche Amministrazioni di fruire ed erogare in maniera concreta sistemi di e-government che sono più dinamici e in grado di soddisfare anche rapidamente le rinnovate esigenze degli utenti finali.

Le stesse PA possono usufruire (e impiegare) di meccanismi che consentono loro di interagire a tutti i livelli di astrazione in maniera più agevole e rapida sfruttando tecnologie basate sempre più su standard e soluzioni aperte. Questo rafforza il requisito di federabilità dei sistemi informativi necessario ad attuare i principi del CAD e a consentire agli utenti finali di esercitare i nuovi diritti previsti dalla norma.

Il modello di riferimento, come accennato all'inizio della sezione 5, consente di aggregare l'erogazione di servizi tanto a livello di Amministrazioni locali, come previsto ad esempio sia dall'art. 16 della Legge 14 Settembre 2011 n. 148 di conversione del decreto-legge 13 Agosto 2011 n. 138, che dall'emananda Carta delle Autonomie in tema di obbligatorietà della gestione associata (mediante Unione di Comuni o Convenzione) nell'esercizio di tutte le funzioni fondamentali dei piccoli Comuni, quanto anche a livello di Amministrazioni centrali. Già oggi forme di aggregazione di servizi sono attive in tali ambiti e costituiscono esperienze spesso di successo. I servizi infrastrutturali in questo disegno costituiscono, a seconda dei casi, i collanti di interoperabilità o i mattoni base che possono favorire la crescita e lo sviluppo di un mercato di servizi per le PA.

Grazie all'uso del modello di riferimento proposto e alle relative soluzioni tecnologiche suggerite, il processo burocratico può concretamente semplificarsi e allo stesso modo innovarsi, presentando agli utenti finali servizi sempre più aggregati e capaci di mascherare le complesse interazioni tra diverse pubbliche amministrazioni. Tali interazioni possono ora risolversi in maniera automatizzata senza un intervento continuo del cittadino o dell'impresa.

Lo snellimento del processo burocratico e il nuovo modello di business promosso dalle soluzioni precedentemente suggerite ha un impatto significativo anche sui costi che possono essere così drasticamente ridotti. Ciò consente una più attenta razionalizzazione delle risorse e una riduzione della spesa pubblica, obiettivi cruciali nell'attuale momento storico di crisi economica che attraversa il nostro paese.

7. CATEGORIE DI SERVIZI

Il disegno del nuovo SPC prevede che siano bandite due tipologie di gara. La prima include tutti i servizi di connettività, sicurezza, calcolo e storage, la seconda invece afferisce a servizi per la realizzazione e l'esercizio di applicazioni per le Pubbliche Amministrazioni. La prima propone servizi che, nell'ambito dei nuovi modelli di servizio SPI, possono essere associati al modello IaaS, la seconda invece fa riferimento a servizi collocabili a livello PaaS e SaaS. Un'esemplificazione dell'insieme di tali servizi è discussa nelle successive sottosezioni.

7.1. Livello SaaS

A livello SaaS della gara applicativa si identificano tutti quei servizi che realizzano la vera e propria logica business delle applicazioni della Pubblica Amministrazione. A tal riguardo, si distinguono due tipi di utenti finali ai quali tali servizi sono rivolti: i cittadini e le imprese, e le Pubbliche Amministrazioni stesse. Le successive sottosezioni elencano gli ambiti di intervento della gara applicativa, distinti per le due tipologie di utenti.

7.1.1. Servizi ai cittadini e imprese

Possono rientrare nella categoria di servizi ai cittadini e imprese i tradizionali siti web e le cosiddette "web apps". A tal proposito, secondo le indicazioni incluse nelle linee guida europee in materia di siti web pubblici, già citate in [1], i servizi web si distinguono in due grosse categorie: *servizi web informativi* e *servizi web evoluti*.

Servizi web informativi: la principale funzionalità offerta da un servizio web informativo è quella di fornire *on-line* all'utente finale tutte quelle informazioni che si rendono necessarie per consentirgli di avviare in forma tradizionale la procedura che porta all'erogazione di un servizio e-government. Essi possono includere sezioni di newsletter in cui fornire informazioni relativamente al servizio di interesse.

Servizi web evoluti: in un servizio web evoluto si deve fornire all'utente finale la possibilità di poter interamente usufruire di un servizio o di servizi aggregati e-government interamente mediante il Web. La sua realizzazione quindi può prevedere:

- l'*accesso* da parte dell'utente al servizio. L'accesso si deve basare su un meccanismo di Single Sign On (SSO) e consente l'uso di strumenti così come definito dagli artt. 64 e 65 del nuovo CAD;
- *sezioni interattive* che guidano l'utente passo passo fino alla erogazione finale del servizio (di base o aggregato). Tali sezioni possono includere (i) *form online* che l'utente può compilare relativamente a un particolare servizio di interesse; (ii) *gestione documenti* attraverso cui l'utente può caricare o scaricare documenti che necessitano di essere esibiti o acquisiti, rispettivamente; (iii) *monitoraggio* dell'evoluzione del servizio (iv) *pagamenti online* attraverso cui l'utente può eseguire il pagamento della transazione.

A contorno di tali funzionalità sezioni interattive possono prevedere l'utilizzo di assistenti virtuali, che assistono l'utente nel compiere i diversi passi per usufruire del servizio e motori di ricerca.

Un'altra categoria di servizi per i cittadini e imprese, che potrebbero anche essere integrati all'interno della categoria di servizi web evoluti, sono i cosiddetti **servizi web pro-attivi.** Nei servizi web pro-attivi, sulla base di un profilo del soggetto, l'Amministrazione informa l'utente sull'insieme di adempimenti che deve effettuare ed eventualmente lo guida precompilando le possibili "richieste" che dovrà inviare all'Amministrazione per poter usufruire di un particolare servizio di interesse.

Queste categorie di servizi possono essere offerte sottoforma di web apps in maniera tale da consentire agli utenti finali di poter utilizzare, in un qualunque momento, tutte le funzionalità precedentemente descritte anche mediante l'uso di dispositivi mobili (e.g., smartphone, tablet). Le web apps possono essere incluse nei siti precedentemente illustrati per il download da parte del cittadino/impresa.

7.1.2. Servizi alle PA

Le Pubbliche Amministrazioni sono la seconda categoria di utenti finali che accedono a un insieme di servizi offerti loro mediante diverse interfacce interattive. Tali servizi consentono di poter realizzare la logica business dei processi amministrativi che possono essere definiti sia all'interno di singole PA, sia nel contesto di uno scenario di federazione di PA che interagiscono tra loro per erogare prestazioni aggregate ai cittadini/imprese.

Pertanto, rientrano in questa categoria per esempio:

- Il servizio **Procedimento amministrativo**: esso comprende quelle funzionalità peculiari di ogni Amministrazione necessarie come presupposto per l'erogazione dei servizi ai cittadini/imprese precedentemente elencati. Le funzionalità come gestione tributi, gestione multe, certificati medici online, gestione SUAP sono esempi di procedimenti amministrativi.

  A supporto di tale servizio, si dovranno definire per esempio:

  - Un servizio di gestione del **protocollo informatico** (art. 40-bis del nuovo CAD)**:** esso consente a una Pubblica Amministrazione di gestire e monitorare tutte le corrispondenze verso sia l'interno che l'esterno che possono generarsi dall'esercizio sia del servizio procedimento amministrativo, sia dei normali procedimenti interni alle PA;
  - Un servizio di gestione del **fascicolo elettronico:** esso consente a una Pubblica Amministrazione di raccogliere tutti gli atti, i documenti e i dati di un procedimento amministrativo (art. 41 del nuovo CAD). Tale servizio può prevedere (i) l'esposizione di taluni dati per la diretta consultazione da parte di altre Pubbliche Amministrazioni nel rispetto delle vigenti disposizioni in materia di privacy (ci si riferisca a tal proposito anche al servizio di gestione di banche dati in rete che può essere utilizzato a supporto per tale scopo) e (ii) la diretta

alimentazione dello stesso sempre da parte di altre PA coinvolte nel procedimento (art. 41 comma 2-bis del nuovo CAD);

- Un servizio di **accesso a banche dati in rete**: i dati delle PA sono raccolti, conservati e resi disponibili e accessibili per l'uso da parte di altre PA e dei privati secondo quanto previsto dall'art. 50 del nuovo CAD. Tale servizio pertanto predispone i necessari meccanismi di accesso a tali banche dati in rete. Il servizio si integra con il sottostante servizio di gestione delle banche dati in rete (si veda la sezione 7.2).

- Il servizio di **sistema collaborativo**: esso deve fornire tutte quelle funzionalità che consentono agli addetti all'interno di una singola Pubblica Amministrazione o agli addetti di Pubbliche Amministrazioni diverse di collaborare tra loro. Esso prevede quindi la possibilità di poter gestire e condividere in maniera unificata idee, documenti, attività e calendari. Il servizio può essere fornito attraverso diverse interfacce (e.g., web, GUIs), o sottoforma di web apps così che siano in un qualunque momento accessibili agli addetti.

7.2. Livello PaaS

Il livello PaaS prevede l'impiego di tutte quelle piattaforme di sviluppo e ambienti run time che consentono la progettazione ed esecuzione dei servizi del livello SaaS. A esse si aggiungono un insieme di servizi integrati con tali ambienti.

Questi servizi includono per esempio:

- Servizio **AAA:** il servizio è progettato e implementato per supportare funzionalità di:
  - *identificazione e Autenticazione* dell'utente volte ad identificare e accertare la corrispondenza tra il soggetto e la sua identità digitale. Vengono supportati tutti e tre i tipi di autenticazione e le loro possibili combinazioni: qualcosa che sai (e.g., password, PIN), qualcosa che hai (e.g., CIE, CNS), qualcosa che sei (e.g., regole biometriche);
  - *Autorizzazione* dell'utente verificando che esso abbia i necessari diritti di accesso a determinate risorse o servizi;
  - *Accounting* attraverso cui tracciare, e quindi generare reportistica, relativamente alle operazioni svolte dai soggetti all'interno di un sistema IT.

Il servizio AAA utilizza meccanismi di Single Sign On (SSO) e si interfaccia con gli elementi SPC infrastrutturali per la gestione federata delle identità digitali.

- Servizio di supporto al **procedimento amministrativo**: possono rientrare in tale servizio per esempio i seguenti elementi:
  - Piattaforma di **Firma e timbro digitale**: è una piattaforma completa per la gestione delle firme e dei timbri digitali. Le sue principali funzionalità potrebbero quindi includere il *timbro digitale*, la *firma automatica semplice, la firma automatica massiva* e *la firma digitale remota (firma digitale as a service)*:
  - **Gestione documentale multicanale**: è un servizio che prevede la gestione di tutti i documenti pervenuti attraverso diversi canali di comunicazione (PEC, email, instant messaging) e riguardanti

i diversi procedimenti amministrativi. Esso potrebbe comprende tutte quelle operazioni che consentono di smistare i documenti ai necessari uffici e di gestire il processo di digitalizzazione di quelli cartacei.

- **Archiviazione/Conservazione dei documenti**: è un servizio che prevede la gestione dell'archiviazione, la conservazione (secondo quanto stabilito dal CAD e dalle regole tecniche in materia di conservazione dei dati e documenti) e il versioning dei documenti. Esso può interfacciarsi con il livello sottostante dei servizi di storage.
- **Servizi di Comunicazione multicanale massiva**: è un servizio che prevede l'invio massivo di documenti o altre comunicazioni sfruttando diversi canali di distribuzione come per esempio, l'email tradizionale, la PEC, gli SMS, l'instant messaging. Il servizio può interfacciarsi con i servizi IaaS sottostanti.
- **PEC evoluta**: è un servizio di gestione di domini PEC evoluti che aggiungono funzionalità quali ad esempio la certificazione dell'identità del mittente del messaggio PEC, l'integrazione automatica con l'IPA.
- **Pagamenti/incassi elettronici**: è il servizio che consente la gestione dei pagamenti ed incassi online. Esso si interfaccia con piattaforme di pagamenti esterne fornite dai "fornitori di servizi complementari" di Figura 1. Così come previsto dalla modifica all'art. 5 del CAD introdotta con la legge n 148 del 14 settembre 2011 che prevede l'istituzione di una piattaforma nazionale condivisa dei pagamenti all'interno del perimetro SPC, tale servizio dovrà interfacciarsi con tale piattaforma.

- **Business Process Management System**: è una piattaforma completa per la gestione dei procedimenti amministrativi. Essa consente la definizione dei processi che costituiscono i diversi procedimenti amministrativi, il controllo delle diverse istanze dei processi (la creazione, l'attivazione, la sospensione e la terminazione), la navigazione tra le diverse attività previste per i processi, l'orchestrazione delle interazioni tra più procedimenti amministrativi e servizi. La piattaforma è sviluppata fornendo un certo numero di interfacce per diverse tipologie di utenti che dovranno quindi autenticarsi per eseguire le operazioni suddette.
- **Governance:** è una piattaforma completa per la governance dei servizi e-government. Essa include:
  - **SLA monitoring**: è un servizio di monitoraggio a run time dei parametri specificati all'interno degli SLA;
  - **Business Intelligence**: è una piattaforma completa per lo sviluppo e la gestione di progetti di Business Intelligence. Esso può includere, per esempio, funzionalità di dashboard, reportistica, analisi multidimensionale OLAP.
- **Gestione banche dati in rete:** è un servizio che consente la gestione a banche dati in rete. Nell'ottica della creazione di servizi evoluti e aggregati per la PA, può essere prevista una gestione federata di banche dati in rete che consenta di (i) specificare quegli opportuni modelli e schemi semantici attraverso cui PA possono definire i dati accessibili in rete (nel rispetto di standard come ISO/IEC 25012), (ii) ricercare dati di interesse, (iii) accedere a tali dati anche ai sensi di quanto previsto dall'art. 58 del nuovo CAD. In quest'ultimo caso il servizio è pienamente integrato con il servizio di accesso a banche dati in rete precedentemente menzionato.

La realizzazione di una federazione di banche dati comporterà un'interazione con i servizi infrastrutturali SPC che dovranno essere previsti per tale scopo.

- **Sicurezza e Privacy as a Service:** è una piattaforma che può essere utilizzata dalle ULS delle PA per poter gestire alcuni aspetti di sicurezza e il coordinamento con il CERT-SPC, parte integrante della governance SPC.
- Servizio di **supporto alla cooperazione applicativa:** tale servizio fornisce due principali funzionalità:
  - *Accordi di servizio*: è un servizio che consente la definizione, la creazione e la pubblicazione di accordi di servizio. La PA utilizza un'interfaccia attraverso cui specificare parametri di alto livello per l'inclusione nell'accordo di servizio. Il servizio ha poi il compito di mappare tali parametri in tutte le parti specifiche tecniche dell'accordo di servizio, che una volta creato viene automaticamente pubblicato nel registro.
  - *Porta di dominio*: è il tradizionale servizio di porta di dominio.

7.3. Ambiti di fornitura: riepilogo

La Figura 5 riepiloga l'elenco degli ambiti di fornitura prima elencati. Si ricorda che il livello IaaS di infrastruttura offre servizi di storage, calcolo, connettività, sicurezza, disaster recovery e business continuità fruibili dalle PA. Tuttavia, come prima sottolineato, tali servizi sono oggetto di un'altra gara (Sezione 2).

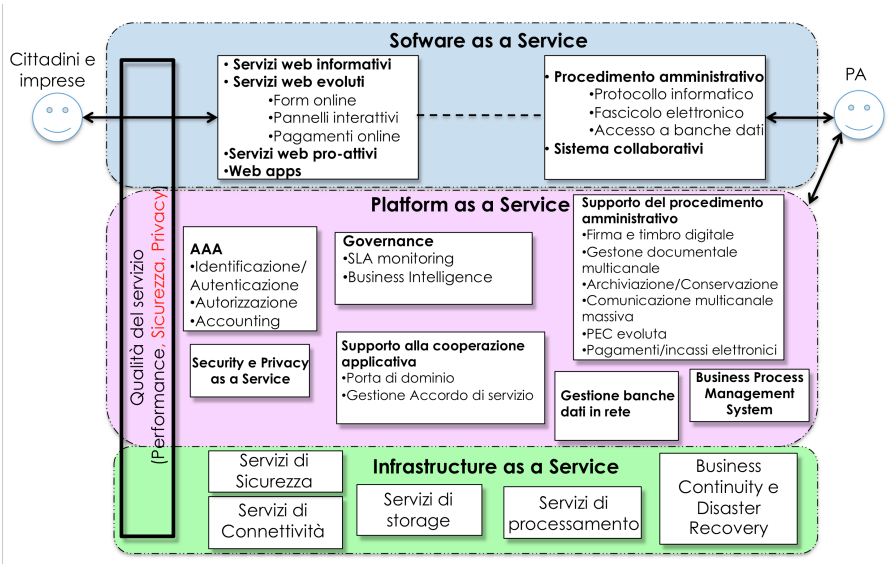

Figura 5: Riepilogo dei diversi ambiti di fornitura identificati per i futuri modelli di servizio SPC

I servizi sopra elencati possono essere corredati di servizi accessori di assistenza e gestione/manutenzione.

7.4. Modello della gara

L'eterogeneità e la dinamicità che emergono dall'introduzione del nuovo modello dei servizi SPC avranno anche un impatto sulla tipologia di procedura da utilizzarsi ai fini dell'individuazione dei fornitori. Un modello di gara che ingessi le tecnologie e non stimoli il ricambio e i benefici dell'innovazione risulterebbe poco efficace. In questa fase le categorie di servizi, pur riferendosi agli ambiti definiti dal CAD e ad un rinnovato e più ricco insieme di regole tecniche, potrebbero avere necessità di integrazione o di definizioni specifiche al contesto della singola PA.

Per le predette ragioni, viste le complessità e gli scenari potenzialmente molto variegati si potrebbe ipotizzare il ricorso all'istituto del confronto competitivo previsto, nell'ambito degli accordi quadro, dal D. Lgs. 163 del 2006. Questo consentirebbe di esprimere al meglio le specifiche esigenze di ciascuna Amministrazione interessata all'acquisizione dei servizi.

Valgono in ogni caso le indicazioni già riportate in [1] riguardanti i diversi strumenti di controllo e monitoraggio da impiegare volti a valutare e verificare che i servizi e i prodotti comunque acquisiti rispondano alle esigenze delle Amministrazioni sia in termini di prestazioni che di qualità.

8. BIBLIOGRAFIA

[1] GdL 3 – Commissione di Coordinamento SPC, "Definizione degli obiettivi delle gare S2 e S3", Settembre 2011

[2] Rif. Documenti GdL DigitPA sul cloud computing